

**Area of Impact: Business and Employment**

1. (a) **Identify *two* other physical characteristics, other than fingerprints, that are currently used in biometric systems.** [2 marks]

Answers may include:

- hand geometry
- iris/retina scanning
- voice recognition
- facial pattern recognition.

*Examiners should be aware that candidates may take a different approach, which if appropriate should be fully rewarded. If in doubt, check with your team leader.*

*Award [1 mark] for each physical characteristic identified up to a maximum of [2 marks].*

- (b) **With reference to the information technology (IT) that underpins biometrics, describe the process of biometric authentication.** [4 marks]

**[1-2 marks]**

*Description of first scanning and storing in database*

- biometric feature is **initially scanned**
- scanned features are **stored in database** together with other personal information.

**[3-4 marks]**

*Description of scanning when in need to authenticate and then matching to features stored in database*

- biometric feature is **re-scanned** when person needs to be authenticated
- scanned feature is **matched** with information in database and if a match then it is authenticated, if no match then it is rejected.

- (c) **Explain why biometric options for payments at retail stores could be considered better than credit card signatures when authenticating the user.**

**[4 marks]**

Sample answer:

“Credit card signatures are open to much fraud. Individuals often lose their credit card, or have it skimmed or stolen. Criminals, who get hold of the credit card, are able to forge the signature. Some criminals don’t even bother to forge the signature as sales people often do not check the signature and, if they do, are often unwilling to confront the card-holder if they have concerns about the signature. Biometrics is considered much more reliable in determining the identity of the card-user. With fingerprint recognition considered about 99% accurate, both customers and shopkeepers feel safe using the system. Signatures are not good at proving the identity of the user – biometrics are.”

*Examiners should be aware that candidates may take a different approach, which if appropriate should be fully rewarded. If in doubt, check with your team leader.*

**[1-2 marks]**

*Describes advantages or disadvantages of biometrics and/or credit card when used for authentication.*

**[3-4 marks]**

*Balanced comparison of biometrics and credit card with a reason at top end of the band.*

- (d) **Discuss the concerns that people might have with the widespread use of biometric technology by several retail stores and different institutions.**

**[10 marks]**

Answers may include:

- identity theft – if the original templates, such as high resolution images of fingerprints, were stolen, they could potentially be used by criminals in an attempt to steal a person's identity
- physical concerns – some people believe that certain biometric technology can cause physical harm or discomfort. Iris/retina scanning may not always be clean, possibly leading to eye disease. People feel very sensitive and protective about their eyes
- privacy – there may be concerns that personal information taken through biometric methods, could be sold to other organizations without the individual's consent or knowledge. The information could be used for a multitude of purposes other than the one for which it was initially intended. This is known as function creep
- erosion of civil liberties – many people believe that a person's anonymity is a fundamental right. If people are forced to use biometric options, for an ID card for example, the 'state' would be intruding into our private lives, with the potential to have control over our everyday activities
- cost to citizens travelling. Biometric passports will cost much more to produce and maintain the records than traditional passport
- reliability – any biometric system is only as good as the initial enrolment system. If someone is improperly registered as a legitimate user, because the initial identification process is flawed, then the whole system is fundamentally flawed. While some biometric applications, like finger recognition, are considered reliable, other options are not and can have an error rate as high as 40%
- policies and standards – unless appropriate policies, standards and laws are developed and enforced, the system is likely to be abused
- Integrity – biometric data, like any IT data, will lack integrity when it has been changed accidentally or tampered with. Because there is human input in the processes problems could occur.

*N.B. Accept examples relating to any reasonable institution or organization, including governments.*

*Examiners should be aware that candidates may take a different approach, which if appropriate should be fully rewarded. If in doubt, check with your team leader.*